БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра многопроцессорных систем и сетей

Аннотация к дипломной работе

«Web – сервис расшифровки файлов»

Гудына Анастасия Геннадьевна

Научный руководитель – старший преподаватель Сакович В.Ю.

2015

РЕФЕРАТ

Дипломная работа, 49 с., 9 рис., 5 табл., 9 источников.

КРИПТОГРАФИЯ, РАСШИФРОВКА ФАЙЛОВ, КРИПТОАНАЛИЗ, WEB-СЕРВИС.

Объект исследования – криптоанализ.

Цель работы - изучить существующие алгоритмы шифрования данных, разработать и реализовать различные алгоритмы расшифровки данных с условием отсутствия какой-либо информации о зашифровке этих данных, разработать и реализовать легко расширяемый Web -сервис расшифровки файлов.

Результатом данной работы является Web-сервис расшифровки файлов, характеризующийся такими свойствами, как многопоточность и легкая расширяемость. Сервис включает разработанные и реализованные алгоритмы зашифровки и расшифровки файлов: моноалфавитная замена, простая перестановка, перестановка строк и перестановка столбцов, AES, Плейфера. Хотелось бы отметить, что алгоритмы расшифровки получают на вход лишь имя файла, необходимого расшифровать.

Реализованный Web-сервис является мощным и гибким средством и может использоваться в сети Интернет.

ABSTRACT

Dyploma work, 49 pages, 9 pictures, 5 tables, 9 sources.

CRYPTOGRAPHY, FILE ENCRYPTION, CRYPTANALYSIS, WEB – SERVICE.

Object of research – cryptanalysis.

Purpose — to explore the purpose and scope of the existing algorithms that used to encrypt data; develop and implement different decryption algorithms in case of complete absence of any information about how file was encrypted; to design and develop easily expandable web – service for file encryption.

The result of diploma work is web – service for file encryption that is characterized by such properties as easily extensibility and multithreading. Service includes developed and implemented encryption and decryption algorithms: monoalphabetic replacement, simple permutation, permutation of rows and columns, AES, Playfair's. It would be better to note that decryption algorithms receive only the file name that should be decrypted.

Implemented Web – service is powerful and flexible resource and can be used in the Internet.